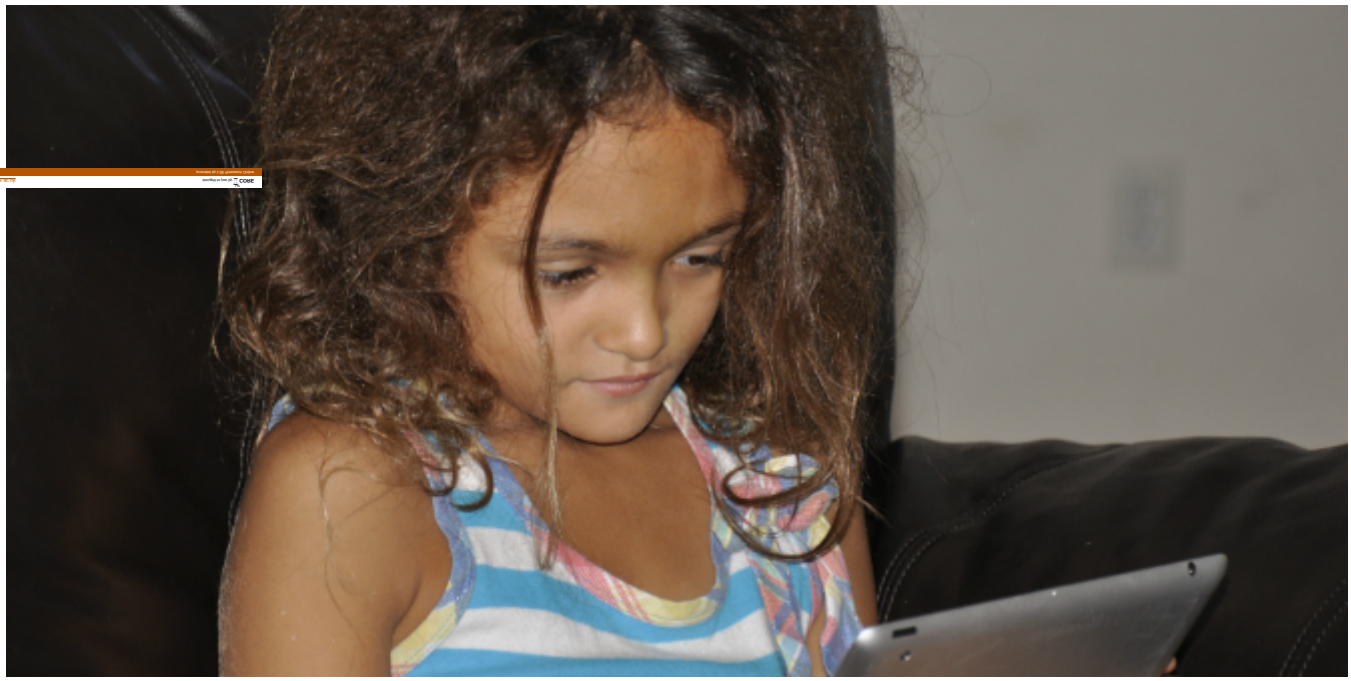
Conceptualising privacy online: what do, and what should, children understand?



Post-Cambridge-Analytica, and post-GDPR, children are becoming increasingly aware of how their data is being used online but there are still limits to their digital literacy. In this post, Sonia Livingstone, Mariya Stoilova and Rishita Nandagiri discuss how they are conceptualising issues of privacy and personal data in their latest ICO-funded research into children's understanding of privacy and data use online. Sonia Livingstone is Professor of Social Psychology in the Department of Media and Communications at the London School of Economics and Political Science. Mariya Stoilova is a Post-doctoral Research Officer on the Global Kids Online project at LSE, and an Associate Lecturer in Psychosocial Studies at Birkbeck, University of London. Rishita Nandagiri is a PhD Candidate at the LSE's Department of Social Policy (Demography and Population Studies) and an external Graduate Associate member of the Centre for Cultures of Reproduction, Technologies and Health, the University of Sussex.

How can social media platforms respect the "best interests of the child" if they don't know which user is a child? How can they meet the needs of children of different ages if the law imposes "bright line" rules – 13+ (COPPA), 16+ (GDPR)? Yet how can society *not* extend hard-won child rights-respecting policy and practice from offline to online? And why should regulators accept low standards of child protection from digital companies?

Such questions have faced policy makers ever since safety risks to children online became evident. They have gained new urgency with the lucrative commercial exploitation of children's data online, along with serious breaches of children's personal information and, in response, the adoption of newly-strengthened privacy legislation.

The European General Data Protection Regulation promises greater protections for the public at large, with specific provisions for children, although challenges remain. The UK is now taking a notable further step. Following intense debate in the House of Lords during the passage of the Data Protection Act 2018, the Information Commissioner's Office (ICO) was charged with introducing an "age appropriate design code" for online providers:

"when they are offering online services and apps that children are likely to access and which will process their data."

In short, privacy-by-design, long called for by civil society, is now on the cards for children. What should it include? What can it add to the ICO's existing guidance on children and the GDPR? The ICO is currently consulting on this, and calling for evidence-based proposals.

Our study

Our ICO-funded project, Children's Data and Privacy Online, is reviewing the evidence on children's conception of privacy online, their capacity to consent, their functional skills (e.g., managing privacy settings) and their deeper understanding of how digital business models influence the uses of personal data. Our literature search located some 10,000 potentially relevant studies, which we have whittled down to the most pertinent. We'll report on the results soon, with a particular focus on children's developing media literacy, by age.

Here we share our conceptual framework for the project, recognising that diverse fields – human rights, regulatory, psychological, sociological, philosophical, technological – all contribute to the understanding of children's data and online privacy. We start with information scientist Helen Nissenbaum's influential definition of privacy as:

"neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information."

This means that privacy depends on the context (itself interesting in the digital environment, with its many and changing apps and services). For our child-rights approach, it valuably sidesteps the popular charge that children (foolishly) either seek or eschew *secrecy*, this in turn seeming to support the popular call on parents to *control* them. Instead, Nissenbaum's notion of privacy as *contextual integrity* prioritises the judgement (especially, by the data subject) of what it is appropriate to share within particular contexts or relationships – particularly important in digital environments where respect for the child's perspective is easily neglected.

But how do children judge what's appropriate to share and with whom or what? How do they conceive the relational contexts in which they and others share their data? Our contention is that children (perhaps adults too) think of privacy most naturally in terms of *interpersonal relationships*, finding it a stretch to think of privacy in relation to commercial organisations or, for different reasons, institutional contexts.

So while they often care deeply about what personal information is shared with their friends or parents, they cannot imagine why the huge corporations which own Instagram or Snapchat, for example, would be interested in *them.* Nor, for different reasons, do they expect to *worry* that trusted institutions (school, doctor) would share their personal information with others, even if digitally recorded in proprietary systems. We suggest that distinguishing *interpersonal, commercial* and *institutional* contexts helps resolve the (somewhat dismissive) privacy paradox – namely that young people *say* they care about their privacy yet in practice they share personal information on public platforms.

As we have heard already in our pilot research with children, they see the point of judging the flow of personal information in interpersonal contexts, because they can influence those. But pragmatically, since children have little agency to affect the take-it-or-leave-it offer of commercial

services, or the over-their-heads management of their data by institutions, they don't generally think of these as *relationships* in which they are engaged as regards their privacy.

In our interviews with children (of which more later), we also heard considerable puzzlement over the idea that their privacy and personal information are *data*. To think about what children know and expect in relation to different types of data, we adapted a typology from privacy lawyer Simone van der Hof, to distinguish:

- 'Data given' – the data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online.
- 'Data traces' – the data left, mostly unknowingly – by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata.
- 'Inferred data' – the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources.

Initial findings

Our findings so far suggest that children are primarily aware of data given in interpersonal contexts. This is largely because they provide that data (though they are aware that their family and friends do too). Their understanding of the consequences for their privacy depends on their developing understanding – depending on age, maturity and circumstance – of interpersonal relationships.

Institutional privacy primarily depends on data given (as collected, for instance, by the School Information Management System) and, increasingly, inferred data in the form of learning analytics or health analytics and the like. Commercial privacy, by contrast, depends heavily on all three types of data.

(Of course we recognise that each form of privacy in one way or another relies on all types of data, and will do so increasingly – but our purpose is to highlight the contrasts between them in terms of main tendencies).

Post-Cambridge-Analytica, and post-GDPR, children are becoming aware of commercial uses of data traces. They know, for instance, that if they search for trainers, they will be served advertisements for trainers thereafter. But their awareness of inferred data and its value to business (or its long-term implications for them personally) is a different matter, and is dependent on their developing understanding of the business models operating in commercial and institutional contexts. This larger understanding – of platform architectures and networked data flows and transactions – is something they are rarely taught about, whatever their age or maturity.

In the absence of an agentic and meaningful relationship with the businesses or institutions that process their personal data, and in the absence of a sufficient critical understanding of the wider contexts within which those businesses or institutions operate, it is likely that children will continue to think of data primarily as data given and privacy in interpersonal terms. The question is how much we can teach children about their privacy in a datafied age and how much those relationships and contexts will instead have to change, if children's right to privacy is to be protected.

This post gives the views of the authors and does not represent the position of the LSE Parenting for a Digital Future blog, nor of the London School of Economics and Political Science

September 6th, 2018 | Featured, In the news, Our publications | 0 Comments